Automated Statechart Model Checking

Dr. Erich Mikk & Paula Pingree
Wednesday, August 28, 2002
12:00 - 1:00 PM
Conference Room 167

Statecharts and auto-code generation are emerging as a powerful approach to implementing software designs for complex missions. This method was used to develop the fault protection (FP) flight software for the Deep Space 1 mission, and has also been adopted for the Deep Impact FP flight software. This technology is generally applicable to flight software components that can be specified as finite state machines.

Proper design validation, which seeks to ensure the correctness of a design at the earliest stage possible, is a major challenge in any software development process. Traditional software validation methods of simulation and testing are being stretched to adequately cover the needs of software development in applications that are growing in complexity. A serious problem with conventional software validation techniques is that one is never sure whether errors still exist in the design. Model checking offers a promising solution for applying a powerful validation technique to mission-critical software. By conducting an exhaustive exploration of all possible behaviors of a software system, model checking can detect design defects that are difficult to discover with conventional testing approaches.

Pingree and Mikk have established a mechanism and process, based on formal methods, for automated translation of statecharts from StateFlow® into Promela, the input language of the Spin model checker, developed by Dr. Gerard Holzmann at Bell Labs. To guarantee compliance with the auto-generated code, the translation tool set preserves the StateFlow® semantics. This permits specification and validation of the design of mission critical software, using the exhaustive exploration techniques of model checking. When the statechart is the source of both the flight code and the Promela model, this automated approach ensures design and validation integrity of the implemented code. In this talk, Mikk and Pingree will describe their work with automating statechart model checking, and their use of the StateFlow® and Promela languages. This work is a joint effort between JPL, Bell Laboratories, and E. Mikk, and is sponsored by JPL's SQI Project.

Dr. Erich Mikk is a Principal Engineer in the Software and Engineering Department of the Siemens Corporate Technology Division in Erlangen, Germany. Currently he is involved in the design and implementation of engineering tools for systems design. Dr. Mikk obtained his Ph.D. degree in 2000 at the Christian-Albrechts University in Kiel. His thesis, titled "Semantics and Verification of Statecharts", establishes mathematical foundations and tool construction for applying model checking to statechart specifications. Prior to completing his degree, Mikk also worked on a research project that applied formal methods and test automation to a design problem at Daimler Benz.

Paula J. Pingree is a Senior Staff Engineer in the Autonomy and Control Section (345) at JPL. She has been involved in the design, integration, test and operation of several flight projects including Mars Observer, Cassini, Mars Global Surveyor, and Deep Space 1. She is currently working on software systems engineering and technology infusion. Pingree holds a Bachelor of Engineering degree from Stevens Institute of Technology in Hoboken, NJ, and an MSEE degree from California State University, Northridge (CSUN). She also teaches part-time in the Electrical & Computer Engineering Department at CSUN.

CSMISS
Center for Space Mission Information and Software Systems

CSMISS IT Spotlight Series: Putting a "spotlight" on Information Technology that is or could be significant to JPL missions.